Altiris Security

Don Kendrick, Senior Manager of Security Operations, VITA

June 5, 2008

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

ALTIRIS OVERVIEW

Altiris

- Business case
- Industry view
- Concerns
- Architecture
- Risk mitigation through ITIL and security controls
- “ Rogue actor” scenario
- Future defense in-depth
- Summary

Questions

Altiris business requirements

- The Partnership is required to centrally manage up to 67,000 desktop/laptop machines and 4500 servers to reduce Commonwealth IT costs and increase security.
- Altiris provides a variety of services to include inventory accounting, software updates and security policy and compliance management
- Altiris is essential to enabling the business success of the VITA contract as VITA consolidates COV Agencies under an enterprise IT governance model
- Altiris IT management through the VITA NG partnership will comply with all ITIL governance processes.

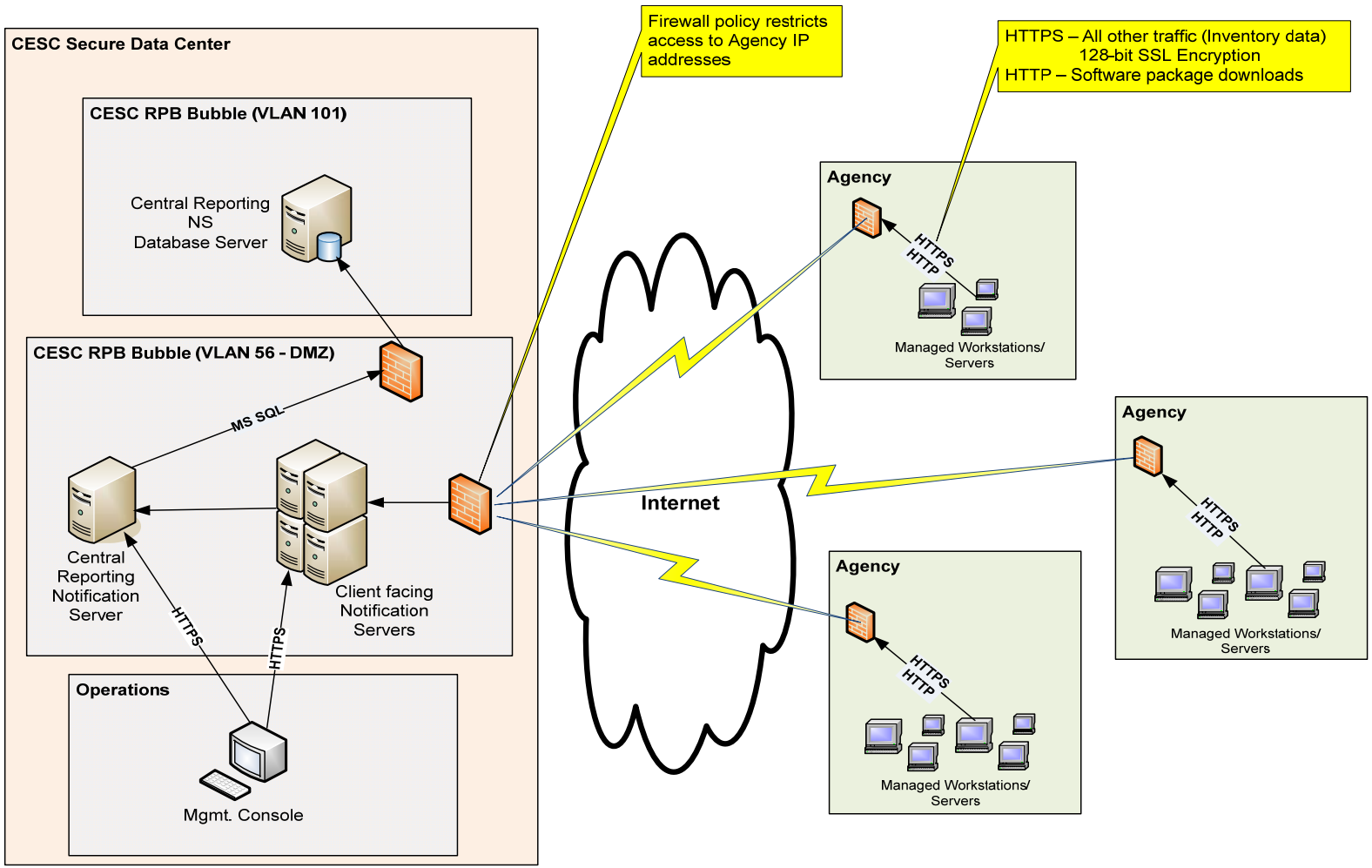
Industry view

REDACTED

Altiris COV concerns

- Too much granular access to a user's machine.
- This access could provide complete machine data knowledge and will enable the administrator to stop services such as security and add and remove programs.
- Rogue administrator could use the Altiris permissions to exploit a user's machine by obtaining unauthorized data or changing the machine configurations that could enable future data exploitation.
- Particular concern centers on Altiris's reported use of the Window's Management Instrumentation (WMI) feature that collects machine data and normally has system administrator level privileges.

Altiris Architecture



Altiris Architecture

Current

- Electronic hardware/software Inventory Collection
- Central Inventory Database
- Deployed to 63,000 Desktop/Laptops and 1,700 Servers

End State

- Electronic Software Delivery
- Patch Management
- Remote Control
  - o Includes enhanced controls to enforce security

Altiris risk position

If we do not deploy Altiris and use the product to provide central IT administration, VITA could incur strategic and operational business risk.

Strategic VITA might not meet its goals to centralize IT management and experience the financial goals for which the partnership was developed.

Operational VITA will not have a standard IT Process that will enable VITA to manage a standard build on Agency machines. A standard build is highly cost effective, significantly lessens the security risk, enables more efficient inventory management systems, and will provide a more efficient platform for future IT initiatives such as virtualization.

Security risk Altiris could present a threat to the confidentiality, integrity, and availability of Agency data. As such, Altiris must have a comprehensive set of security and monitoring controls that significantly reduce the risk associated with an Altiris deployment.

Risk mitigating controls

Altiris IT Governance

Altiris management will comply with all ITIL Service Delivery Governance requirements

- Service request management
- Incident management
- Software asset management
- Problem management
- Configuration management
- Change management
- Release management
- Security management

Risk mitigating controls

Security controls governing Altiris

Physical security

- Altiris servers are secured within the CESC data center
- Administrators receive Altiris access after background checks and drug screens are completed

Logical security

- Altiris servers are connected to a restricted network within the RPB bubble
- Except for software package downloads, all data flows between the Altiris console and the managed end-point occurs via an encrypted SSL communication channel

Risk mitigating controls

Security controls governing Altiris

Access control

Windows- access control environment

- Windows Administrator has access to everything within Windows
- No restrictions on the account built-in to Windows
- Local logging of actions only
- Possible to “cover your tracks” by clearing security log

Altiris-access control management

- Altiris initial rights granted within Active directory
- Altiris then restricts rights with granular permissions for Altiris technician
- Altiris technician does job without windows administrative rights
- Centralized logging of administrator actions
- Central logging increases degree of difficulty to “cover your tracks”

Risk mitigating controls

Security controls governing Altiris

Operational and Security Monitoring

- CSIRC monitors key technologies (such as Altiris/Symantec) and alerts Service Delivery personnel when updates are ready.
- Updates are applied according to Partnership SLAs
- ESOC provides comprehensive incident response coverage

Auditing

- All audit logging within the infrastructure applies to Altiris activity
- Altiris has its own protected central logging feature. Can not be erased by the local system administrator as can window logs
- If a windows administrator changed host level configurations manually at each workstation or server, there would be no audit trail **….. Altiris fixes this situation**

Risk mitigating controls

Security controls governing Altiris

Data protection

- Altiris uses SSL communication when communicating with the host.
- Altiris uses SQL data base to store all permissions, clients, and asset inventory
- Altiris audit logs and security controls stored in database
- No direct access to database – logs cannot be tampered

Risk mitigating controls

Security controls governing Altiris

Comparison of Windows Management Instrumentation (WMI) and Altiris

- There are key differences between the two products
- Altiris uses a proprietary agent for computer management

- **WMI (Windows Management Instrumentation)**
  - Inherent in Windows 2000 and newer OSs
  - Used by many Windows applications including Altiris
  - Provides remote management capabilities
  - By default, requires administrator rights to access remotely

- **Altiris and WMI**
  - Altiris agent does not install or modify WMI on managed device
  - Altiris does not use WMI remotely
  - Altiris agent uses WMI locally for collecting inventory information
  - Altiris reduces exploitation of WMI by minimizing staff with Windows Admin rights

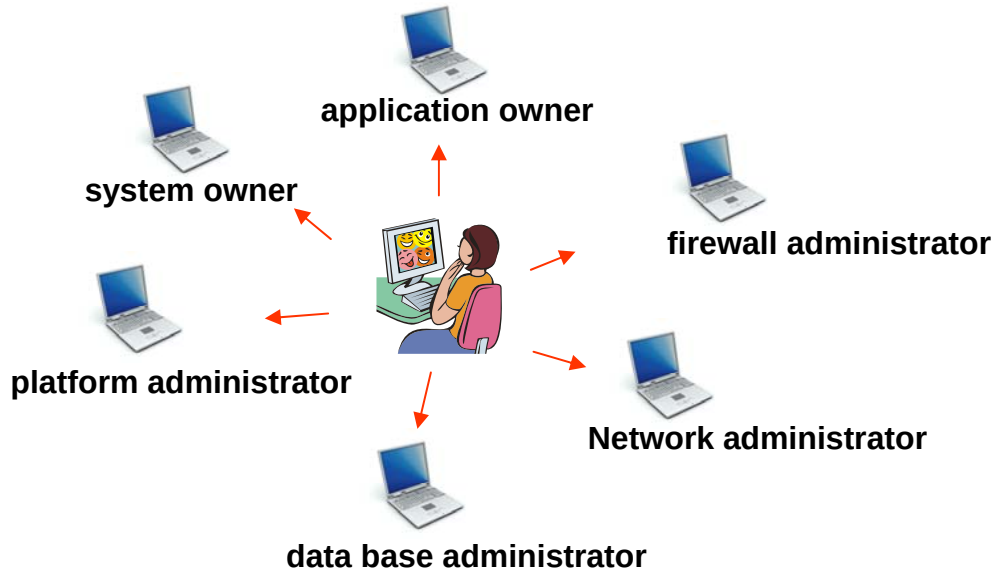
Rogue actor mitigation

Centrally controlled environment

- 24 x 7 infrastructure monitoring
- Defense in-depth
- Extensive personnel background checks and drug testing of potential Altiris technicians
- Limited access. Altiris provides for distribution of limited "administrative rights" to support inventory management without granting total access to the systems
- Discovery and Accountability through improved logging capabilities More granular than windows and logs centrally stored within Altiris
- CSIRC/ESOC integration (after transformation) for better response capabilities
- Enforcement through alignment with HR policies (disciplinary actions)
- COV, VITA Partnership and NG Program Security Office oversight
- IT governance through ITIL

Altiris checks and balances

Pre partnership



Post partnership

- data base administrator
- platform administrator
- system owner
- application owner
- network administrator

- data center manager
- Altiris administrators
- ESOC
- firewall administrator

The issue under post partnership is that COV Agencies might not know these people

Altiris checks and balances II

Environment Oversight and control

Partnership trust

- Highly respected corporation working with great COV employees for the citizens of Virginia

Access control

- Granular system restrictions based on roles and functions to be performed on a server or work station. For example, an Altiris admin DOES NOT have Windows admin privileges

Separation of duties (SOD)

- Given the information on last slide, SOD is more defined than ever before. Access control methods defining rights and privileges restricted to admin designated function

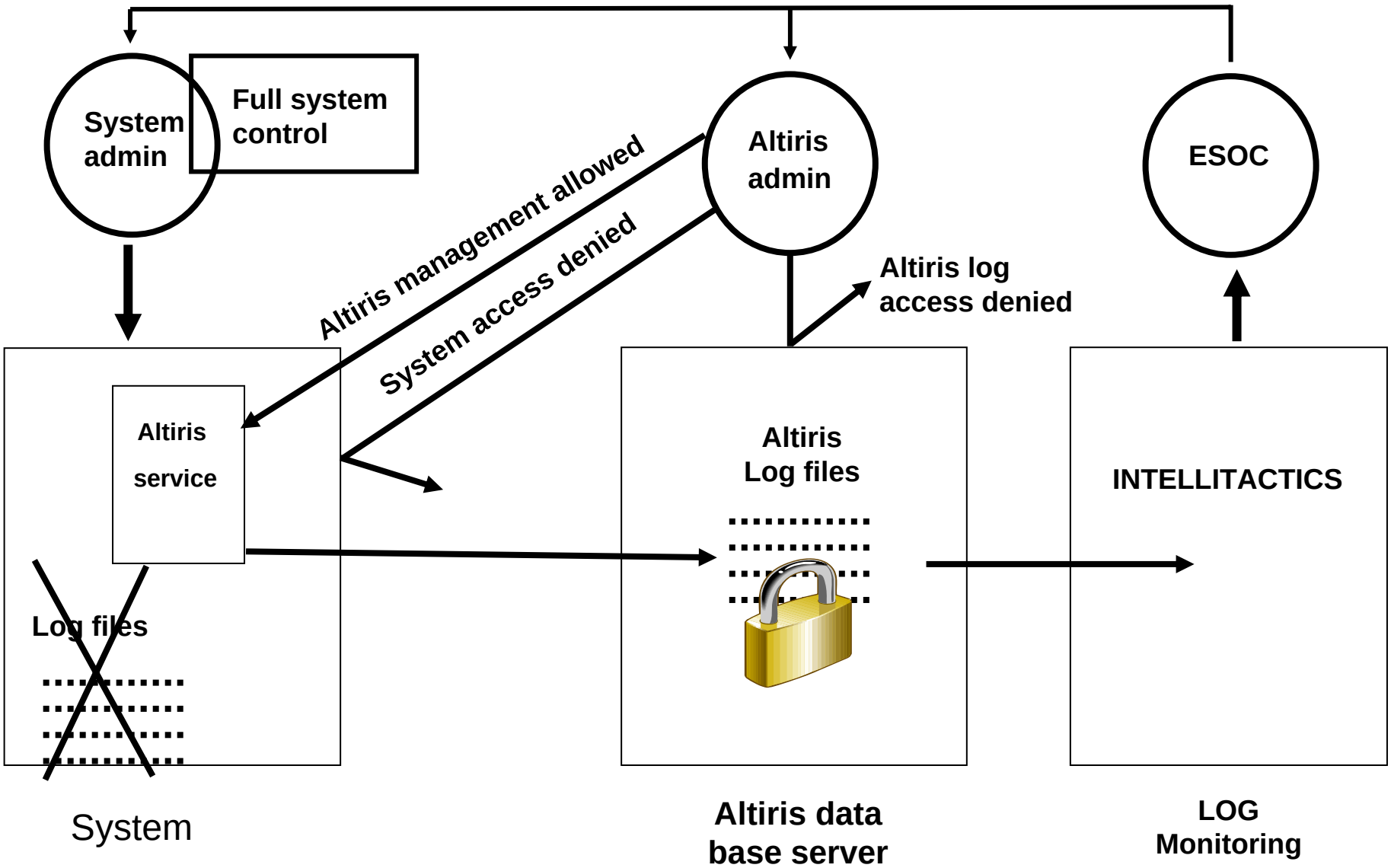
Monitoring, logging and auditing

- User actions logged using native platform logging and additional technical means
- ESOC monitors information 24x7x365 for anomaly indicators, breach detection, and policy violation
- Altiris security expressions will ensure compliance to VITA security standards
- Pen tests and vulnerability scanning will reveal weaknesses
- Extensive external auditing

Staffing

- Extensive background checks and highly skilled talent
- Numerous prior COV employees

Sys admin vs Altiris admin rights



Future security posture

REDACTED

Defense in-depth

REDACTED

Summary

Altiris

- Strategic and key VITA business solution
- Deployed on very limited basis to assist transformation
- Represents state of the art IT solution
- Operated within ITIL governance umbrella
- Platform and Altiris security controls protect user data
- Altiris does not directly employ WMI
- Future Altiris security posture will grow as additional Altiris functions deployed

QUESTIONS